DeviceLock

Comment combattre les fuites de données via les réseaux sociaux ?

Tribune d'Alexei Lesnykh
Responsable du Développement International et
de la Stratégie Produit de DeviceLock

En France, selon l'Ifop, 77% des internautes se déclarent membres d'au moins un réseau social. La moyenne s'établit à 2,8 réseaux sociaux auxquels un internaute français appartient. Outre la baisse de productivité des salariés et la consommation de bande passante réseau ou encore l'exposition à des contenus inappropriés, comme le confirme une récente enquête du Ponemon Institute, l'utilisation des réseaux sociaux en entreprise accentue deux types de menaces : les infections par des virus ou autres codes malveillants et les fuites d'informations confidentielles. S'il est clair que les logiciels antivirus peuvent atténuer efficacement les risques de malwares, la menace de fuite de données n'est pas très bien prise en compte et les scénarios spécifiques liés aux réseaux sociaux sont mal compris. Nombre de responsables de la sécurité des systèmes d'information (RSSI) se demandent en fait comment combattre cette menace.

Réseaux sociaux en entreprise, je t'aime moi non plus

Pour de nombreuses entreprises, les réseaux sociaux sont devenus un outil essentiel au service de la plupart de leurs processus métiers. Les interactions avec ses réseaux, tant en interne qu'à l'extérieur, peuvent servir à construire l'image de marque, améliorer la réputation de la société, fidéliser la clientèle, recruter des talents, mobiliser les connaissances collectives des collaborateurs, raccourcir le cycle de développement ou bien optimiser la réactivité du support technique. En effet, les responsables RH recherchent des candidats sur LinkedIn et XING, les équipes de R&D publient leurs guides de développement sur des wikis d'entreprise et l'équipe du support technique emploie la messagerie instantanée pour discuter en temps réel des problèmes critiques concernant un produit. Même le CRM, de par sa nature intrinsèque, s'appuie sur un ensemble de communications sociales profilées en fonction des besoins spécifiques de l'activité.

En parallèle, les progrès incroyables de l'électronique grand public ont conduit à une consumérisation de l'informatique dans les entreprises, où les salariés ont tendance à apporter leurs propres équipements. Le phénomène du Bring Your Own Device rend donc l'utilisation des réseaux sociaux inévitables. Il est quasi impossible d'empêcher vos collaborateurs de poster sur des blogs, de « chatter » et de consulter leurs réseaux sociaux favoris à partir de leur ordinateur portable ou smartphone personnel tout en l'utilisant à des fins professionnelles.

Cependant, les avantages que les médias sociaux apportent aux entreprises vont de pair avec divers problèmes. Le système d'information peut rapidement être infecté lorsque les salariés téléchargent des fichiers et données sur les ordinateurs qu'ils utilisent dans le cadre de leur travail. Les fuites de données peuvent se produire accidentellement ou délibérément lorsque des informations sensibles pour l'entreprise sortent de son réseau interne.

Avant tout, une charte d'utilisation des réseaux sociaux est une condition préalable à leur sécurisation dans un environnement d'entreprise. Cependant, les erreurs, la curiosité, la négligence et autres écarts font inéluctablement partie de la nature humaine. Par conséquent, même la meilleure des chartes risque d'être souvent enfreinte. C'est pourquoi, aux côtés des mesures organisationnelles, les RSSI doivent choisir et déployer une solution de sécurité capable de prévenir avec efficacité la fuite de données sensibles de l'entreprise, depuis les postes de travail via les profils personnels et professionnels des salariés sur les réseaux sociaux. La difficulté est de le faire sans bloquer entièrement l'accès aux sites et services, car cela aurait une incidence négative sur la productivité et le moral des collaborateurs.

Une seule solution : la DLP

La solution passe par la différenciation des informations personnelles, professionnelles, publiques et confidentielles dans les échanges sur les réseaux sociaux. Elle doit donc être orientée données et reconnaître les contenus. En outre, pour que les communications sociales légitimes (c'est-à-dire conformes à la charte relative aux réseaux sociaux) ne soient pas affectées, la solution retenue doit prendre des décisions et les appliquer immédiatement. Cela implique l'utilisation de méthodes d'analyse de contenu en temps réel. Parmi les nombreuses technologies existantes de sécurité informatique, la seule qui réponde véritablement à l'ensemble de ces critères est la *prévention des fuites de données* (DLP, *Data Leak Prevention*).

Face au grand nombre de solutions DLP aujourd'hui disponibles sur le marché, le choix de la plus efficace pour sécuriser les réseaux sociaux dans une entreprise dépend principalement des critères suivants. Tout d'abord, il faut trouver un équilibre entre l'éventail des services que l'entreprise doit contrôler et la couverture des réseaux sociaux assurée par une solution DLP. En règle générale, il vaut mieux que la solution en question contrôle le plus de services possible. Elle doit au moins couvrir les réseaux sociaux et services de messagerie instantanée les plus répandus, à savoir Google+, Facebook, Twitter, LinkedIn, XING, LiveJournal ainsi que Skype, ICQ/AOL, Windows Live Messenger, Jabber, IRC et Yahoo! Messenger.

Un autre critère tout aussi important concerne le degré de contrôle que la solution DLP offre sur les divers canaux de fuite de données, en fonction de l'utilisation que l'entreprise fait des réseaux sociaux. Par exemple, les communications sociales des salariés, à partir de leur poste de travail au bureau pour des échanges au sein de l'entreprise ou sur Internet, peuvent voir leur contenu contrôlé par des passerelles DLP implantées à la périphérie du réseau d'entreprise. Dans le même temps, en raison de l'omniprésence des réseaux sans fil modernes, l'utilisation de terminaux mobiles (smartphones, tablettes et ordinateurs portables), fait craindre un scénario catastrophe. En effet, le terminal d'un salarié, qu'il soit sa propriété ou celle de l'entreprise, même utilisé au bureau, peut facilement contourner non seulement la sécurité de périmètre, mais aussi l'ensemble du réseau de l'entreprise en se connectant à des réseaux mobiles 3G, voire à des bornes d'accès WiFi extérieures situées à proximité. Tout cela s'applique aussi lors d'une utilisation à distance, que ce soit en voyage, chez un client ou à domicile.

L'incapacité des solutions de sécurité, résidant sur le réseau, à contrôler les communications des mobiles signifie que les entreprises doivent mettre en place des mesures de contrôle des réseaux sociaux directement sur les terminaux à protéger au moyen d'agents logiciels DLP. Fonctionnant sur le terminal, l'agent DLP analyse et filtre le contenu de tous les échanges sur les réseaux sociaux en fonction de la charte de sécurité de l'entreprise, quels que soient le lieu et le moyen de connexion à Internet ou au réseau de l'entreprise.

Toutefois, dans le cas des smartphones et tablettes reposant sur le système Android ou iOS, le contrôle des réseaux sociaux n'est aujourd'hui pas aussi simple que sur les ordinateurs portables Windows ou Mac. Il est en effet actuellement impossible d'installer des agents DLP sous Android et iOS sans « jailbreaker » (modifier illégalement) le système d'exploitation, ce qui constitue une méthode inacceptable pour la sécurité informatique de l'entreprise. En revanche, dans les années à venir, plusieurs solutions de sécurité innovantes en mode cloud devraient faire leur apparition sur le marché pour protéger les données des entreprises contre les fuites sur les réseaux sociaux, à partir des smartphones et tablettes.

Au moment d'évaluer le niveau de couverture des médias sociaux par une solution DLP, il ne faut pas oublier que les réseaux sociaux les plus fréquentés, tels Google+, Facebook ou Twitter, ainsi que les messageries instantanées emploient des méthodes de cryptage standard (par exemple HTTPS ou FTPS) ou propriétaires (à l'image de Skype) pour sécuriser les communications réseau entre le terminal et le site Web du réseau social ou le poste de l'interlocuteur. Il est crucial que les agents DLP installés sur les terminaux puissent intercepter ces communications de manière à extraire les données transférées en clair afin d'en filtrer le contenu. Dans certains cas, cette interception ne peut s'effectuer que sur le terminal, et non sur la passerelle DLP. C'est notamment le cas lorsqu'il s'agit de contrôler le contenu des messages instantanés cryptés par Skype.

Une autre fonctionnalité essentielle pour assurer la couverture de tous les canaux empruntés par les réseaux sociaux est la capacité pour l'agent DLP de contrôler les communications réseau qui transitent par des proxies HTTP et SOCKS. Souvent, ces proxies sont utilisés par les utilisateurs ou configurés automatiquement et, si l'agent DLP présent sur le terminal ne peut intercepter et analyser les communications passant par leur intermédiaire, cela crée un risque non maîtrisé de fuite de données entrantes ou sortantes, et accroît nettement le risque d'infection par un malware.

Conclusion

Donc, une fois que la couverture des réseaux sociaux et l'exhaustivité du contrôle des canaux DLP sont garanties, la solution DLP choisie préviendra avec fiabilité les fuites de données via les communications sociales. En outre, grâce à un filtrage des types de données permettant de bloquer le téléchargement de code exécutable à travers les réseaux sociaux, les solutions DLP peuvent également réduire les risques d'infection par des malwares.

A propos d'Alexei Lesnykh :

Responsable du développement international et de la stratégie produit de DeviceLock, Alexei Lesnykh a rejoint la société en 2007. Avec plus de 10 ans d'expérience en sécurité informatique, son expertise s'étend à de multiples domaines : la sécurité des réseaux, les infrastructures publiques, la gestion de l'authentification et de l'identification ainsi que la voix sur IP et le calcul virtuel. Avant de rejoindre DeviceLock, Alexei Lesnykh était analyste indépendant, contribuant au développement de stratégies d'entreprises et de produits et travaillant à la mesure des risques d'investissement pour le compte de sociétés internationales. Ses expériences précédentes l'ont conduit à prendre part au développement à l'international de start-up russes : TrustWorks Systems B.V. ou ELVIS-PLUS, par exemple. Alexei Lesnykh est titulaire d'un Master en sciences informatiques obtenu à l'institut des technologies électroniques de Moscou.

À propos de DeviceLock, Inc. :

Depuis sa création en 1996 sous le nom de SmartLine, DeviceLock, Inc. fournit des solutions logicielles de contrôle et de protection des informations en entreprises de toutes les tailles et tous les secteurs d'activité. Avec plus de 4 millions d'ordinateurs protégés dans plus de 60 000 organisations de par le monde, DeviceLock compte une vaste clientèle institutionnelle, parmi laquelle des établissements financiers, des organismes publics nationaux et fédéraux, des réseaux militaires classés, des prestataires de soins de santé, des entreprises de télécommunications et des établissements scolaires. DeviceLock, Inc. est une société internationale comptant des agences à San Ramon (Californie, États-Unis), Londres (Royaume-Uni), Ratingen (Allemagne), Moscou (Russie) et Milan (Italie).

Contact presse :
Mediasoft Communications – Carole Scheppler
Carole.scheppler@mediasoft-rp.com - 01 55 34 30 00

###